WINSIGHT

# Observabilidade para operações confiáveis

Monitoramento de infraestrutura, rede, aplicações e serviços críticos em uma única central.

**APRESENTAÇÃO INSTITUCIONAL**

Curitiba 2026

# O desafio operacional

**Quando cada parte da infraestrutura é acompanhada separadamente, a equipe descobre muitos problemas depois que o usuário já sentiu o impacto.**

| | | |
|---|---|---|
| **01** | **Visibilidade fragmentada** | Estações, servidores, rede, links e serviços ficam distribuídos entre ferramentas e verificações manuais. |
| **02** | **Diagnóstico demorado** | Sem correlação e histórico, a equipe perde tempo para localizar a causa provável e medir o impacto. |
| **03** | **Ação reativa** | Alertas genéricos geram ruído, enquanto falhas críticas podem chegar tarde ou sem contexto suficiente. |

# Uma central para acompanhar toda a operação

**O WinSight reúne sinais técnicos e organiza a resposta em uma visão única por empresa, unidade e equipamento.**


**Alertas com contexto • histórico • auditoria • orientação para correção**

# Cobertura da plataforma

A solução acompanha a infraestrutura do ponto de vista técnico e operacional.

| Camada | O que acompanha | Decisão apoiada |
|---|---|---|
| **Equipamentos** | CPU, memória, disco, tráfego, disponibilidade e inventário | Capacidade, manutenção e priorização |
| **Rede** | Descoberta, topologia, interfaces, latência, perda e utilização | Localização de gargalos e falhas |
| **Internet** | Link principal e contingência, operadora, qualidade e histórico | Continuidade e evidência para provedores |
| **Serviços e aplicações** | Processo, serviço esperado, consumo, ausência e indisponibilidade | Proteção daquilo que sustenta a operação |
| **Incidentes** | Regras por equipamento, confirmação, deduplicação e recuperação | Resposta com menos ruído e mais contexto |

# Da coleta à ação

Um fluxo simples transforma telemetria em prioridade operacional.

**1**

## Coleta

Agent e Probe observam equipamentos e rede com baixo volume de dados.

**2**

## Correlação

A central preserva identidade, histórico e contexto por empresa e unidade.

**3**

## Regra

Limites e tempo de confirmação filtram picos e condições transitórias.

**4**

## Resposta

O incidente nasce com impacto, evidência e orientação para a equipe.

**Resultado: a equipe recebe menos alertas repetidos e ganha evidência para decidir mais rápido.**

# Saúde, capacidade e inventário

**Cada equipamento mantém uma identidade operacional mesmo quando o endereço IP muda.**

- Uso de CPU, memória, armazenamento e tráfego
- Disponibilidade, heartbeat e histórico por período
- Fabricante, tipo, hostname, MAC e histórico de IP
- Orientação técnica para gargalos e risco de indisponibilidade

**CAPACIDADE**

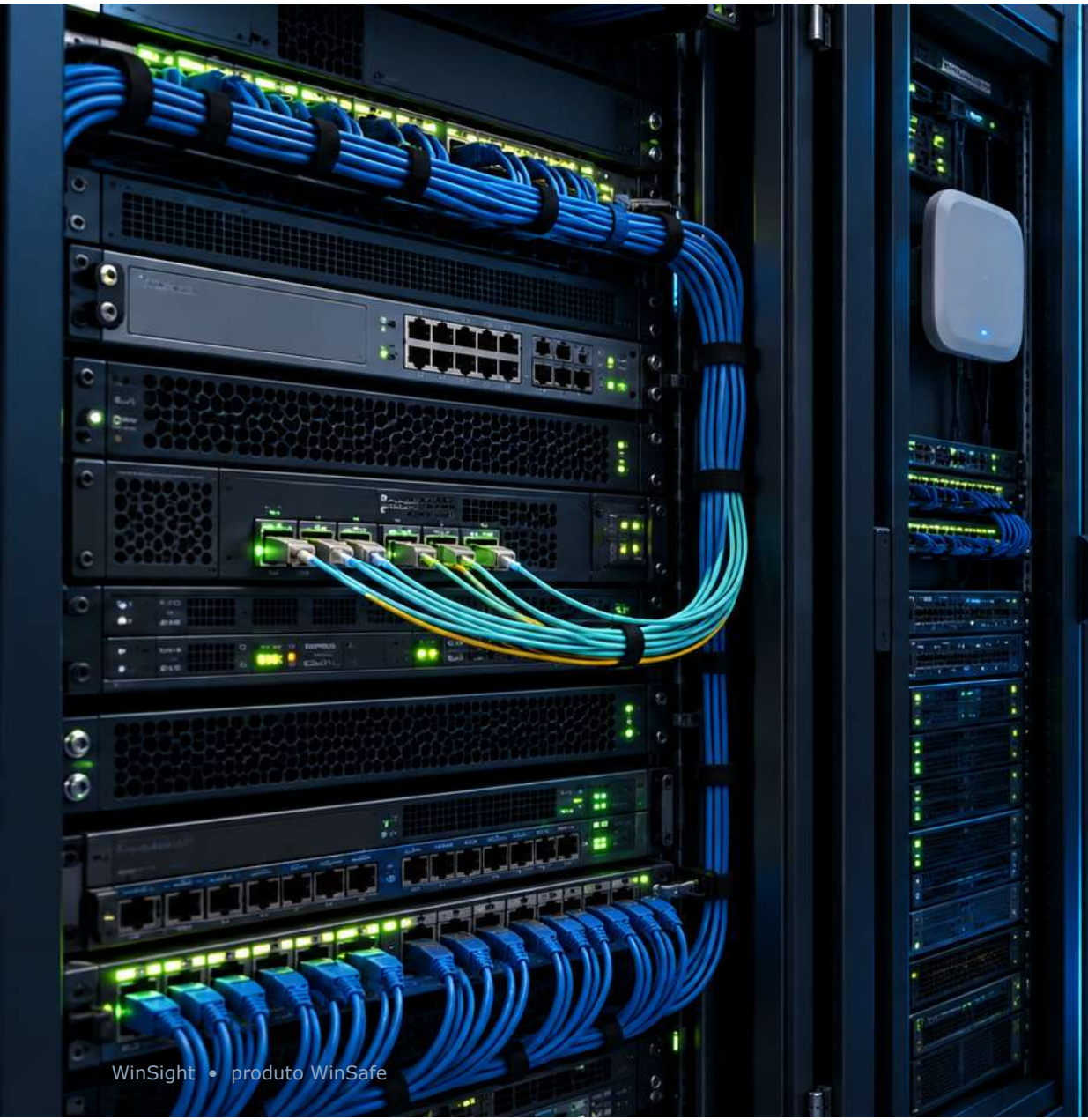
**Antecipar saturação antes do impacto**

**INVENTÁRIO**

**Saber o que existe e onde está**

**HISTÓRICO**

**Comparar comportamento e confirmar causa**



# Rede e links de internet

- Descoberta de equipamentos e visão da topologia
- Latência, perda, disponibilidade e utilização
- Link principal, contingência e terceiros
- Integração com roteadores, firewalls e SNMP somente leitura
- Histórico para investigar gargalos e cobrar operadoras

A profundidade da telemetria depende dos equipamentos e integrações aprovadas pela TI.

# Aplicações e serviços críticos

**O monitoramento deixa de tratar todos os processos como iguais e concentra atenção no que sustenta a operação.**

**SERVIÇOS ESSENCIAIS**

- Banco de dados e backup
- Antivírus e serviços do Windows,Windows Server e Linux
- Impressão, integrações e aplicações internas

**PERFIS DE APLICAÇÕES**

- Processo ou serviço esperado por equipamento
- Limites de CPU e memória
- Detecção de ausência, falha e consumo elevado

**Resposta automática:** confirma a condição, abre uma ocorrência única, acompanha a normalização e preserva o histórico.

# Alertas com contexto e menos ruído

**CONDIÇÃO**

Limite por equipamento ou aplicação

**CONFIRMAÇÃO**

Persistência mínima antes do incidente

**CORRELAÇÃO**

Uma ocorrência para o mesmo problema

**RECUPERAÇÃO**

Encerramento quando o ambiente normaliza

**A equipe recebe o problema consolidado, o equipamento afetado, o impacto provável e a evolução até a recuperação.**

E-MAIL PAINEL HISTÓRICO

# Segurança e governança

## O desenho de operação plena combina isolamento, controle de acesso e rastreabilidade.

| | |
|---|---|
| **IDENTIDADE** | Perfis de proprietário, administrador, operador e visualizador. MFA e licenciamento integrados ao WinSafe Core. |
| **ISOLAMENTO** | Dados e ações segregados por empresa, com validação de autorização em todas as operações. |
| **AGENTS E PROBES** | Tokens com ciclo de vida, rotação, revogação, expiração e proteção contra repetição indevida. |
| **AUDITORIA E PRIVACIDADE** | Registro de ações, política de retenção, acesso mínimo necessário e adequação à LGPD. |

A apresentação não expõe detalhes de implementação, endpoints, segredos ou mecanismos internos de proteção.

# Aplicação sugerida

## O piloto pode começar pelo ambiente que mais concentra risco operacional e expandir após a validação.

| | | |
|---|---|---|
| 01 | **Infraestrutura** | Servidores, estações e armazenamento |
| 02 | **Rede** | Switches, fibra, gateways e pontos de acesso |
| 03 | **Segurança física** | NVR, câmeras e equipamentos conectados |
| 04 | **Continuidade** | Links de internet e serviços essenciais |
| 05 | **Operação** | Alertas, histórico, responsáveis e auditoria |

**Escopo final definido em conjunto com a TI, respeitando acessos, criticidade e políticas internas.**

# Piloto controlado e evolução por evidência

**A implantação reduz risco ao validar cobertura, alertas e rotina da equipe antes da expansão.**

**01**

### Descoberta

Inventário, criticidade, integrações permitidas e critérios de sucesso.

**02**

### Baseline

Coleta inicial, comportamento normal e ajustes de identificação.

**03**

### Operação assistida

Regras, alertas, serviços críticos e validação conjunta com a TI.

**04**

### Expansão

Novas unidades, ativos e integrações conforme resultado do piloto.

**Critérios sugeridos: cobertura dos ativos prioritários, qualidade dos alertas, tempo de diagnóstico e adesão da equipe.**

# Resultados esperados

- Identificação mais rápida da causa provável
- Menos indisponibilidade percebida pelo usuário
- Prioridade clara para a equipe técnica
- Histórico para decisões, auditoria e fornecedores
- Visão consistente entre unidades e responsáveis

**O valor do piloto será medido com os critérios definidos.**

WINSIGHT

PRÓXIMA DECISÃO

# Aprovar o escopo técnico do piloto

Uma reunião entre WinSafe define ativos prioritários, integrações autorizadas, responsáveis e critérios de sucesso.

**Workshop técnico** | **Plano do piloto** | **Início da coleta** | **Revisão dos resultados**

www.winsafe.com.br

Escopo, integrações e níveis de serviço sujeitos à validação técnica e proposta comercial.